LWE From Non-Associative Cyclic Division Algebras

Sven Bootsma [2], Bor de Kock [2], Valeriy Malikov [1,2], Ekin Özman [1], Jaap Top [1]

[1]University of Groningen [2]TNO

Boxed name denotes main author (master's thesis); remaining authors are supervisors

From LWE to NCLWE

With the expected advent of quantum computers compromising classical cryptographic schemes, lattice-based cryptography has emerged as a leading candidate for quantum-secure cryptography. The **Learning With Errors (LWE) problem** is the most prominent construction:

Sample $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ uniformly, a small error $e \leftarrow \psi$, fix $\mathbf{s} \in \mathbb{Z}_q^n$ and output

$$(\mathbf{a}, b) = (\mathbf{a},\ \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$$

Write m many samples as matrix-vector multiplication:

$$(A, A\mathbf{s} + \mathbf{e} \mod q) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$$

Given polynomially many samples:
Search Problem: Find $\mathbf{s}$.
Decision Problem: Distinguish samples from uniformly random ones.
Hardness is based on hardness of worst-case lattice problems (e.g. **GapSVP**).

Let K a (cyclotomic) number field, $\mathcal{O}_K$ its ring of integers. Replace $\mathbb{Z}_q^n$ by $\mathcal{O}_K/q\mathcal{O}_K$ to increase efficiency.

Variant	Sample space	Storage/sample	# LWE samples
LWE	$\mathbb{Z}_q^n$	$O(n^2)$	n
RLWE	$\mathcal{O}_K/q\mathcal{O}_K$	$O(n)$	n
MLWE	$(\mathcal{O}_K/q\mathcal{O}_K)^d$	$O(dn)$	nd
NCLWE	$\Lambda/q\Lambda$	$O(dn)$	nd^2

Why structure helps: Ring elements admit a matrix representation via left-multiplication on a fixed basis: e.g. for $a \in \mathcal{O}_K$,

$$\mathrm{vec}(a \cdot s) = C(a)\,\mathrm{vec}(s)$$

with

$$C(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

allowing efficient storage and multiplication.

In MLWE, d such blocks $C(a_{1,1}), \ldots, C(a_{1,d})$ are concatenated; giving a $n \times nd$ block matrix.

Caveat: Structure that helps efficiency can also help an attacker, an issue partly motivating MLWE from RLWE.

The Race for Efficiency: Can We Do Better?

RLWE wraps n LWE samples into one structured sample; MLWE wraps d RLWE samples into one.

Can we wrap d MLWE samples into one, the same way? Maybe — using a **non-associative cyclic division algebra**.

Let K be a degree n number field, L/K cyclic Galois of degree d with $\mathrm{Gal}(L/K) = \langle \theta \rangle$, and $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$. Define an auxiliary element u subject to $u^d = \gamma$, $xu = u\theta(x)$, and set:

$$\mathcal{A} = (L/K, \theta, \gamma) = L \oplus uL \oplus \cdots \oplus u^{d-1}L$$

Key fact: Since $\gamma \notin K$, $\mathcal{A}$ is *non-associative*:
$(u \cdot u^{d-1}) \cdot u = \gamma u = u\theta(\gamma) \neq u \cdot (u^{d-1} \cdot u) = u\gamma$

Non-Associative Cyclic LWE (NCLWE)

Replace the ambient space in MLWE $\mathcal{O}_K^d$ by the natural order $\Lambda = \bigoplus_{i=0}^{d-1} u^i \mathcal{O}_L$. Sample $a \leftarrow \Lambda/q\Lambda$, fix secret $s \in \Lambda^\vee/q\Lambda^\vee$ and small error e; output

$$(a, b) = (a,\ (a \cdot s)/q + e \bmod \Lambda^\vee)$$

Analogous search/decision problems and worst-case security reduction.

Left multiplication by $a = a_0 + a_1 u + \cdots + a_{d-1}u^{d-1}$ on the basis $\{1, u, \ldots, u^{d-1}\}$ gives

$$\phi(a) = \begin{pmatrix} a_0 & \gamma\theta(a_{d-1}) & \cdots & \gamma\theta^{d-1}(a_1) \\ a_1 & \theta(a_0) & \cdots & \gamma\theta^{d-1}(a_2) \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & \theta(a_{d-2}) & \cdots & \theta^{d-1}(a_0) \end{pmatrix}$$

One algebra element a encodes a $d \times d$ matrix using only d ring elements — saving a storage factor of d over MLWE.

The necessity of non-associativity:
An analogous construction was given for $\gamma \in \mathcal{O}_K$. The resulting algebra is then associative and nicer to work with. However, this required a restriction on the element s which potentially compromises security.

The price of non-associativity:
The map $\phi : \mathcal{A} \to M_{d \times d}$ is no longer multiplicative: $\phi(as) \neq \phi(a)\phi(s)$ in general. This single fact drives every issue (and contribution) on the right. A lot of the background machinery needed to be adapted.

Contribution 1: A PKE Scheme, At a Cost

Let $d = [L : K] = 2$, $\gamma \in \mathcal{O}_L \setminus \mathcal{O}_K$ and set $\mathcal{A} = (L/K, \theta, \gamma) = L \oplus uL$.

Building a public-key encryption scheme from NCLWE: Due to $\phi(\cdot)$ being non-multiplicative, **decryption leaves a residual term**

$$\phi(as)^T - (\phi(a)\phi(s))^T = \begin{pmatrix} 0 & 0 \\ 0 & (\theta(\gamma) - \gamma)a_1\theta(s_1) \end{pmatrix}$$

that cannot be rounded away — but it only appears in the second row.

Fix: Encrypt the message twice (once plain, once reversed/re-indexed) and keep only the clean upper half from each. This works, but **degree d appears to require d such encryptions, making the efficiency gain insignificant in practice.**

Proof idea: First, an elaborate correctness proof of the double encryption construction. Then, a proof of independence of both samples and a security tie to the hardness of NCLWE.

Contribution 2: An Impossibility at Higher Degree

Proving security requires the existence of a second algebra $\mathcal{A}' = (L/K, \theta, \gamma')$ with matrix representation ϕ' such that for every $a \in \mathcal{A}$, there exists some $a' \in \Lambda'$ with $\phi(a)^T = \phi'(a')$.

Theorem. For $d \geq 3$, no such non-associative $\mathcal{A}'$ exists.

Proof idea: Matching entries of $\phi(a)^T$ and $\phi'(a')$ forces $\gamma = \theta(\gamma)$, i.e. $\gamma \in K$, contradicting non-associativity. Even allowing $\mathcal{A}$ associative leads to further contradictions.

This rules out the original method for proving security for *any* $d \geq 3$, regardless of the choice of γ'.

Outlook

- A security proof in the case of $d \geq 3$ needs a fundamentally different strategy.
- Is there *any* PKE or other scheme where non-associativity is not an efficiency obstruction in practice?

References

[1] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)*, 60:1–23, 05 2010.

[2] Andrew Mendelsohn and Cong Ling. Learning with errors from nonassociative algebras. *IACR Communications in Cryptology*, 1, 01 2025.

[3] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), September 2009.

Valeriy.malikoff@gmail.com